DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/28/2010 has been entered. Claims 5-8, 19 and 21 have been canceled. Claims 1-4, 9, 10, 12, 14, 16, 18 and 20 have been amended. Independent claim 28 and dependent claims 22-27 have been added. Claims 1-4, 9-18, 20 and 22-28 are now pending.

Specification

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The Examiner notes that claim 1 recites a tracing protocol however applicant's specification paragraph 68 of applicant's original disclosure recites a discrepancy -tracing procedure. Additionally the Examiner notes in paragraph 86 of applicant's specification the Examine notes that the applicant recites a back-tracing procedure. As such the Examiner notes that it is difficult to interpret applicant's claim 1 tracing protocol.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 12, 14, 16 and 18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The Examiner notes that the claim is directed to “computer program”. The Examiner notes that the MPEP states that a “computer program” not resident to some form of “computer readable medium” is considered to be non-statutory subject matter. Additionally the Examiner notes that the “medium” must not contain transitory signals.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 10 -14 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fujioka et al. (US Patent No. 6,845, 447 and Fujioka hereinafter) in view of Jorba et al. (US Patent Publication No. 2005/0021479 and Jorba hereinafter).

1. As to claims 1, 10 -14 and 28, Fujioka teaches a electronic voting method, comprising the steps of: obtaining from a signer apparatus, according to a fair blind signature scheme (i.e.,. ..teaches the use of a blind signature scheme [abstract., lines 1-7],

a digital signature (yi) of a data signal (xi) generated from a voter apparatus (i.e., …teaches generating a digital signature [col. 5, lines 25-30] and a encrypted vote (e.g., data signal) [col. 5, lines 15-25]), said data signal comprising an encrypted vote (vi) of a voter (i.e.,...teaches a encrypted vote [col. 5, lines 15-25]; and establishing, at a trusted authority apparatus, a link between a data pair (xi, yi) comprising said data signal and said digital signature (i.e., …teaches (zi, yi) where zi is the encrypted vote and yi is the signature [col. 5, lines 46-50]),

and a signing session in which said data pair (xi, yi) was generated (i.e., …teaches generating a (zi, yi) where zi is the encrypted vote and yi is the signature [col. 5, lines 46-50]),

With regards to applicant's claim limitation of the fair blind signature scheme permitting establishment of the link via a tracing protocol included in the fair blind signature scheme, the applicant is noted to disclose in paragraph 18 the following: :"… fair blind signature schemes enable a given digital signature to be linked to a given user". While Fujioka is noted to teach a blind signature scheme, Fujioka teachings do not expressly disclose permitting establishment of the link via a tracing protocol included in the fair blind signature scheme. In this instance the Examiner notes the teachings of Jorba. Jorba is noted to a teach blind signature voting scheme comprising a verification protocol (e.g., tracing protocol) where a link ballot identifier is used for tracability purposes. See Jorba paragraph 123. Therefore given the system described above by Fujioka, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance process integrity by employing Jorba's verification protocol as described above.

2. As to claim 2, the system of Fujioka disclose the use of a fair blind signature scheme, however the system does not expressly teach voting method where the fair blind signature scheme comprises a threshold fair blind signature scheme in which the digital signature is generated by cooperation of a number t of n servers, where t n, and where n - t + 1 servers need to be honest. However in this instance the Examiner notes the teachings of Jorba. Jorba is noted to discloses in paragraph 7 the following: " A cryptographic voting scheme accurately determines the steps and actions involved in the remote vote casting as well by the device issuing the votes used by the voter as by the corresponding voting server. The scheme also determines the cryptographic operations which must occur during the process of vote tallying and also for verifying the final results. Of course, a cryptographic voting scheme must also be completed with generic safety measures to maximise the safety and to best protect the full voting system. Therefore given the system described above by Fujioka, a person of ordinary skill in the art would have recognized the advantage of modifying a system to

enhance process integrity by employing Jorba's verification protocol as described above.

5-8 (Cancelled).

3. Claims 3, 15-18 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fujioka in view of Jorba as applied to claim 1 above, and further in view of Juang et al. (NPL " A Verifiable Multi-Authority Secret Election Allowing Abstention from Voting.(Juang hereinafter) (cited from IDS (date 9/15/2006)).

4. As to claims 3 and 22, Fujioka teaches a voting method where the data signal (x/) corresponds to the encrypted vote (vi) of the voter which is encrypted according to a first encryption scheme (ErM) (i.e., …teaches encrypted vote [col. 5, lines 15-25]),

With regards to applicant's claim limitation of:

said first encryption scheme being the encryption scheme of a first mix-net (TM) contained in a vote-tallying module, the Examiner notes that neither Fujioka nor Jorba discloses the elements as recited in the above claim limitation. However in this instance the Examiner notes the teachings of prior art Juang specifically paragraph 3.3. Juang is noted to teach the use of mix-net in a voting process. Therefore given the system described above by Fujioka and Jorba, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance data security by employing Juang 's mix-net process as described above.

5. As to clams 15 and 16, Fujioka teaches a voting system ballot-order-randomizer module comprising a processor configured to provide:

input means for receiving a batch of cast votes, each cast vote comprising an encrypted data signal (ci) comprising data (xi) indicative of a respective vote (vi) of a voter which is digitally signed according to a fair blind signature scheme (i.e.,. ..teaches the use of a blind signature scheme [abstract., lines 1-7] …further teaches generating a digital signature [col. 5, lines 25-30] and a encrypted vote (e.g., data signal) [col. 5, lines 15-25])),

each encrypted data signal (ci) being encrypted according to a predetermined encryption scheme (EM) [col. 5, lines 15-25]);

With regards to applicant's claim limitation of, “said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated”, the applicant is noted to disclose in paragraph 18 the following: :”… fair blind signature schemes enable a given digital signature to be linked to a given user”. While Fujioka is noted to teach a blind signature scheme, Fujioka teachings do not expressly disclose permitting establishment of the link via a tracing protocol included in the fair blind signature scheme. In this instance the Examiner notes the teachings of Jorba. Jorba is noted to teach a blind signature voting scheme comprising a verification protocol (e.g., tracing protocol) where a link ballot identifier is used for tracability purposes. See Jorba paragraph 123. Therefore given the system described above by Fujioka, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance process integrity by employing Jorba's verification protocol as described above.

and output means for outputting the decrypted signals of said batch of cast votes in an order different from the order of corresponding encrypted data signals in said batch of cast votes (i.e…. the Examiner notes fig 5 of Fujioka where Fujioka illustrates a decryptor and outputting the decrypted encrypted vote signals).

The combined teachings of Fujioka and Jorba are noted to teach decrypting a encrypted data signal (e.g. vote) by applying a decryption scheme. See figure 5 of Fujioka. However the combined teachings of both references do not expressly teach applicant's usage of a mix-net as recited in applicant’s claim limitation element “a mix-net (M) for decrypting said encrypted data signals (ci) by applying a decryption scheme (DM) which is an inverse of said predetermined encryption scheme (EM); However in this instance the Examiner notes the teachings of prior art Juang specifically paragraph 3.3. Juang is noted to teach the use of mix-net in a voting process. Therefore given the system described above by Fujioka and Jorba, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance data security by employing Juang 's mix-net process as described above.

6. As to clams 17 and 18, Fujioka teaches a voting system ballot-order-randomizer module comprising a processor configured to provide:

input means for receiving a batch of cast votes, each cast vote comprising an encrypted data signal (ci) comprising data (xi) indicative of a respective vote (vi) of a voter which is digitally signed according to a fair blind signature scheme (i.e.,. ..teaches the use of a blind signature scheme [abstract., lines 1-7] …further teaches generating a digital signature [col. 5, lines 25-30] and a encrypted vote (e.g., data signal) [col. 5, lines 15-25])),

each encrypted data signal (ci) being encrypted according to a predetermined encryption scheme (EM) [col. 5, lines 15-25]);

With regards to applicant's claim limitation of, “said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated”, the applicant is noted to disclose in paragraph 18 the following: :”… fair blind signature schemes enable a given digital signature to be linked to a given user”. While Fujioka is noted to teach a blind signature scheme, Fujioka teachings do not expressly disclose permitting establishment of the link via a tracing protocol included in the fair blind signature scheme. In this instance the Examiner notes the teachings of Jorba. Jorba is noted to teach a blind signature voting scheme comprising a verification protocol (e.g., tracing protocol) where a link ballot identifier is used for tracability purposes. See Jorba paragraph 123. Therefore given the system described above by Fujioka, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance process integrity by employing Jorba's verification protocol as described above.

The combined teachings of Fujioka and Jorba are noted to teach decrypting a encrypted data signal (e.g. vote) by applying a decryption scheme. See figure 5 of Fujioka. However the combined teachings of both references do not expressly teach applicant's usage of a mix-net as recited in applicant’s claim limitation element “a mix-net (M) for decrypting said encrypted data signals (ci) by applying a decryption scheme (DM) which is an inverse of said predetermined encryption scheme (EM); However in this instance the Examiner notes the teachings of prior art Juang specifically paragraph 3.3. Juang is noted to teach the use of mix-net in a voting process. Therefore given the system described above by Fujioka and Jorba, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance data security by employing Juang 's mix-net process as described above.

19 (Cancelled).

21 (Cancelled).

Allowable Subject Matter

Claims 4, 9, 20 and 23-27 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

Examiner Remarks – Specification Objection

The Examiner withdraws the objection made to the specification in view of claim 4 in view of applicant's amendment. The objection made in view of claim 7 is withdrawn due to the cancellation of claim 7.

Examiner Remarks - 35 U.S.C. §112, first paragraph –Claim 6

The Examiner withdraws the rejection made under 112 for claim 6 in view of the claim cancellation.

Examiner Remarks - 35 U.S.C. §103(a),

Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Flynn Nathan can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2431